G. GRABARNIK ET AL.
YOR20030326US1 (GHZ)

FIG.1

FIG.2

210 ~

File   Options   Help

messageStart

messageEnd

separator

...

220 ~

rule1
rule2
rule3

ComponentId: Application Server ProcessId: 3840 ThreadId:
SourceId: com.ibm.ws.webcontainer.http.HttpTransport ClassName:
Manufacturer: IBM Product: WebSphere Version:
ServerName: test1 TimeStamp: 2003-05-13 16:31:32.3630
Severity: 3 Category: AUDIT PrimaryMessage: SRVE
9080. ExtendedMessage:

260 ~

Link Down.
(Link Down).
(Link) Down.
Link (Down).

SE 5.0.0 s0245.04]

port http on port

230 ~   Log Viewer

240 ~   Rule Building View

250 ~   Result Viewer

FIG.3

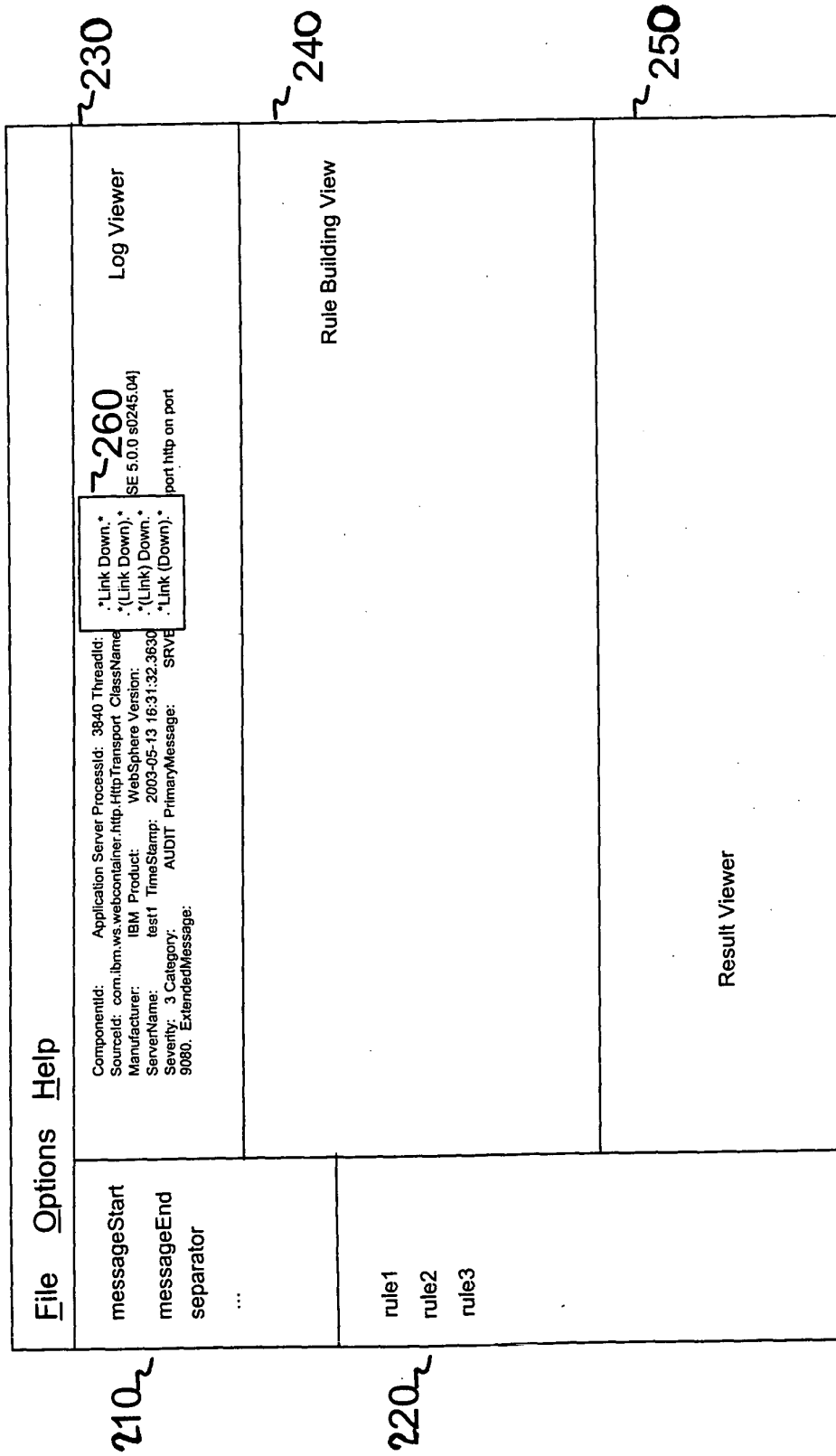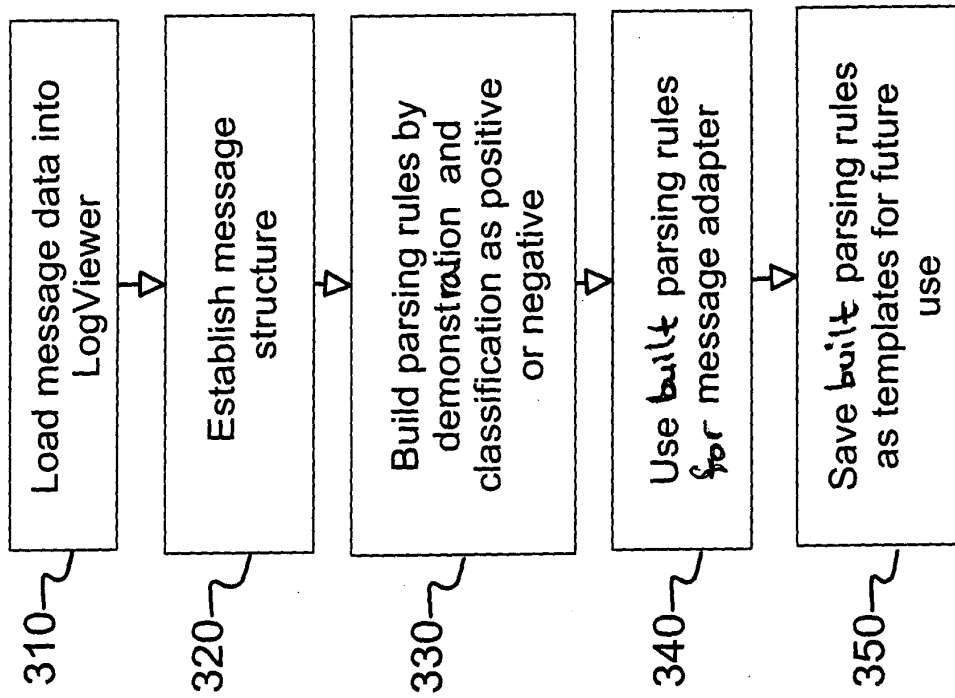|	
310	Load message data into LogViewer
320	Establish message structure
330	Build parsing rules by demonstration and classification as positive or negative
340	Use built parsing rules for message adapter
350	Save built parsing rules as templates for future use

FIG.4

```
<?xml version="1.0" encoding="UTF-8" ?>
<schema targetNamespace="http://MsgStructure.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <element name="MsgStructure">
        <complexType>
            <attribute name="multiline" type="boolean"
default="false"/>
            <attribute name="eventStart" type="string"/>
            <attribute name="eventEnd" type="string"/>
            <attribute name="separator" type="string" default="\s+"/>
            <attribute name="msgType" type="MsgTypeType"/>
            <attribute name="glueing" type="string" default=","/>
            <attribute name="matchContinue" type="string"/>
        </complexType>
    </element>
    <simpleType name="MsgTypeType">
        <restriction base="NCName">
            <enumeration value="TEC_RECEPTION_MSG" />
            <enumeration value="DB2_MSG" />
            <enumeration value="WAS_ACTIVITY_LOG" />
            <enumeration value="WAS_MSG" />
            <enumeration value="UNKNOWN_MSG" />
        </restriction>
    </simpleType>
</schema>
```
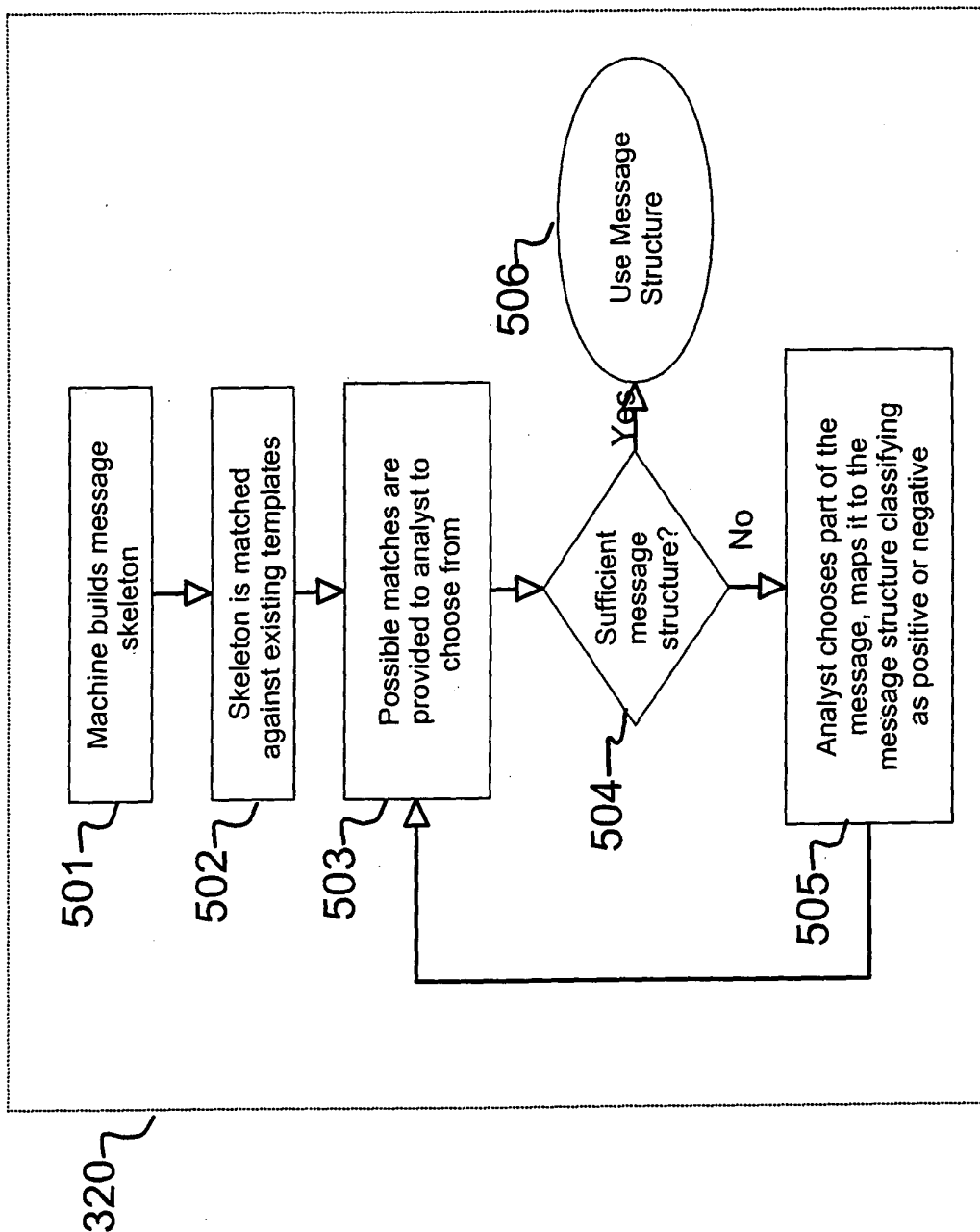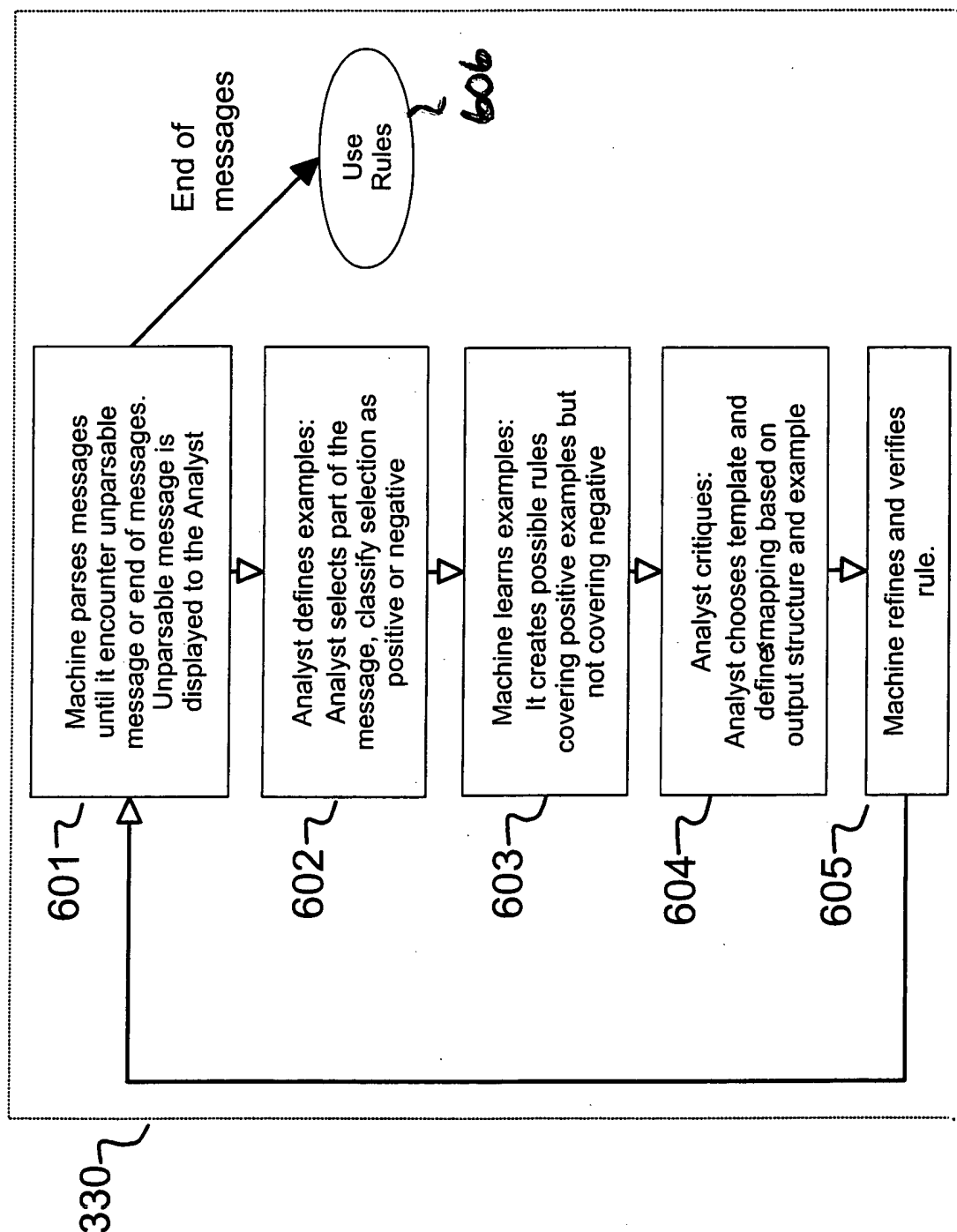
400

FIG.5

320

| 501 | Machine builds message skeleton |

| 502 | Skeleton is matched against existing templates |

| 503 | Possible matches are provided to analyst to choose from |

504 — Sufficient message structure?

Yes → 506 — Use Message Structure

No →

| 505 | Analyst chooses part of the message, maps it to the message structure classifying as positive or negative |

FIG.6

330

601 — Machine parses messages until it encounter unparsable message or end of messages. Unparsable message is displayed to the Analyst

End of messages →

606 Use Rules

602 — Analyst defines examples: Analyst selects part of the message, classify selection as positive or negative

603 — Machine learns examples: It creates possible rules covering positive examples but not covering negative

604 — Analyst critiques: Analyst chooses template and defines mapping based on output structure and example

605 — Machine refines and verifies rule.

FIG.7

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<schema targetNamespace="http://OutputStructure.xsd">
  <element name="OutputStructure">
    <complexType>
      <sequence>
        <element ref="Fields" maxOccurs="unbounded" />
      </sequence>
      <attribute name="separator" use="required" type="string" />
      <attribute name="hashing" use="optional" type="string" />
    </complexType>
  </element>
  <element name="Fields">
    <complexType>
      <sequence>
        <element ref="GroupsMsgDataElement" minOccurs="0" maxOccurs="1" />
        <element ref="RuleAttCreationTime" />
        <element ref="RuleAttSeverity" />
      </sequence>
      <attribute name="Match" type="string" />
      <attribute name="Substitute" type="string" />
      <attribute name="Split" type="string" />
      <attribute name="Name" type="string" />
      <attribute name="Description" type="string" />
    </complexType>
  </element>
  <element name="RuleAttCreationTime">
    <complexType>
      <sequence>
        <element ref="Subs" minOccurs="1" maxOccurs="unbounded" />
      </sequence>
      <attribute name="Value" type="string" use="optional"/>
    </complexType>
  </element>
  <element name="Subs">
    <complexType>
      <attribute name="Positions" type="string" />
      <attribute name="Match" type="string" />
      <attribute name="Substitute" type="string" />
      <attribute name="TimeFormat" type="string" />
    </complexType>
  </element>
</schema>
```
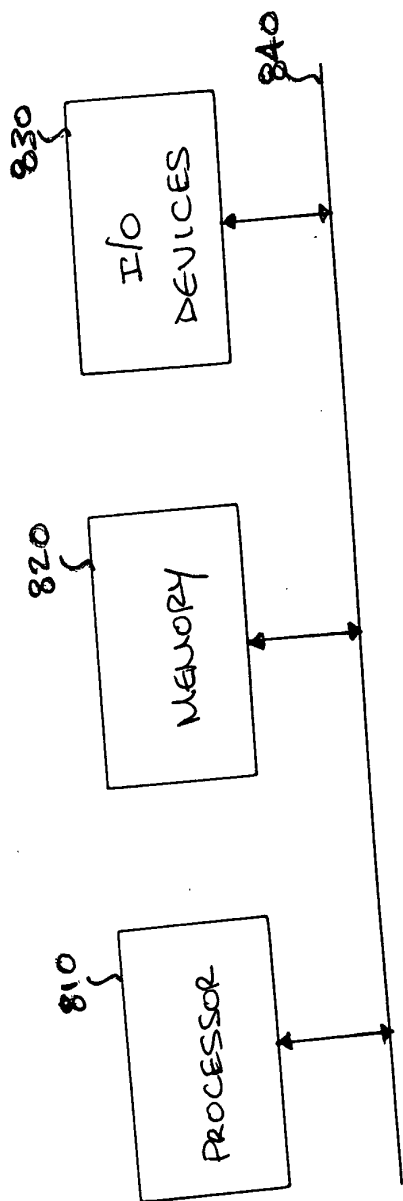
700

FIG. 8